IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MoneyGram Payment Systems, Inc., *Plaintiff,* v. Capgemini America, Inc., *Defendant.*	Case No. _____

PLAINTIFF MONEYGRAM PAYMENT SYSTEMS, INC.'S
ORIGINAL COMPLAINT

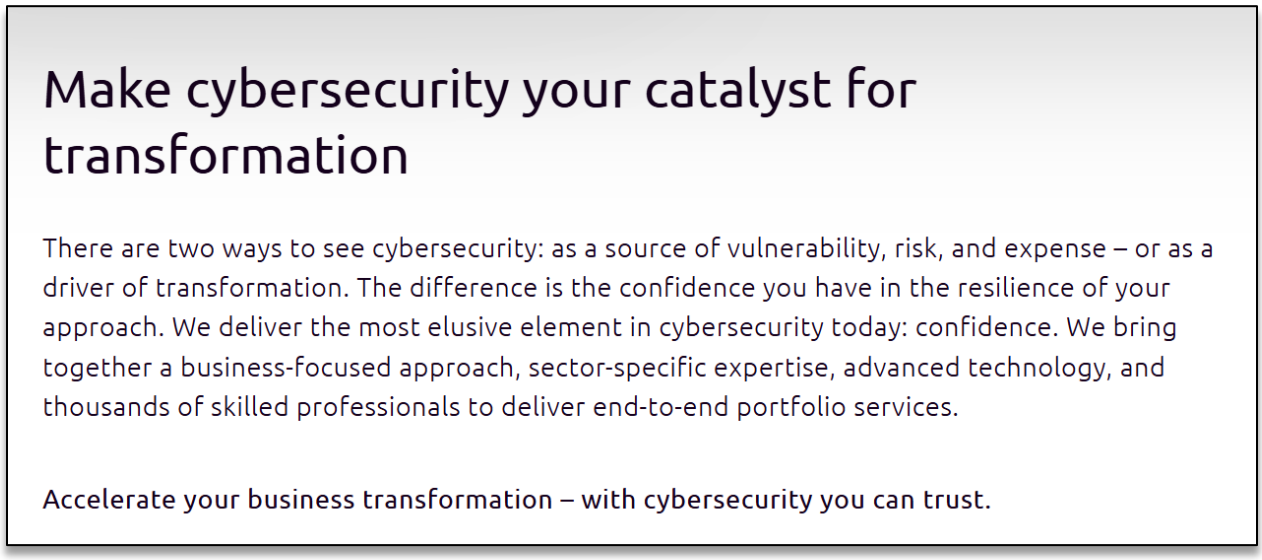
Plaintiff MoneyGram Payment Systems, Inc. ("MoneyGram") files this Original Complaint ("Complaint") against Defendant Capgemini America, Inc. ("Capgemini").

I. NATURE OF SUIT

1. MoneyGram is a global payments company operating in over 200 countries and territories around the world. MoneyGram's innovative cross-border platform provides millions of consumers globally the ability to send money home for family and friends to pick up in cash or receive directly to a bank account, mobile wallet, or card. With over 440,000 retail locations and five billion digital endpoints, MoneyGram provides one of the most robust digital and physical money movement networks in the world. With over five billion digital endpoints, cybersecurity is critical to MoneyGram and its consumers.

2. Capgemini holds itself out as "a global leader in technology services" that "offers integrated solutions for digital transformation, blending expertise with cutting-edge technology." Capgemini claims to be a leading expert in cybersecurity. In fact, Capgemini assures its customers

that it provides its customers with "confidence" and "trust," such that cybersecurity should not be viewed as source of vulnerability or risk:[1]



Make cybersecurity your catalyst for transformation

There are two ways to see cybersecurity: as a source of vulnerability, risk, and expense – or as a driver of transformation. The difference is the confidence you have in the resilience of your approach. We deliver the most elusive element in cybersecurity today: confidence. We bring together a business-focused approach, sector-specific expertise, advanced technology, and thousands of skilled professionals to deliver end-to-end portfolio services.

Accelerate your business transformation – with cybersecurity you can trust.

3. Relying on Capgemini's representation that it was an industry leader who could be trusted with a company's most sensitive data, MoneyGram hired Capgemini to perform certain IT related services. The parties entered into a Business Services Master Agreement ("MSA") and Statement of Work ("SOW") that govern the services Capgemini agreed to provide, including a service desk to which MoneyGram personnel could call to handle technical inquiries. On September 20, 2024, a Capgemini service desk analyst permitted an unauthorized third party ("Unauthorized Third Party"), impersonating various MoneyGram employees across multiple phone calls, to reset MoneyGram employees' user credentials and thereby gain access to MoneyGram's network, causing MoneyGram to cease money transfer operations for several days and leading to the unauthorized access and acquisition of personal data belonging to MoneyGram customers (the "Data Incident").

[1] https://www.capgemini.com/services/cybersecurity/.

4. The Data Incident, caused entirely by Capgemini's failure to stop an obvious fraudster from accessing MoneyGram's network, has caused MoneyGram millions of dollars in damages. MoneyGram was forced to completely shut down its entire global business for six days, causing significant loss of revenue and harm. Additionally, MoneyGram has incurred and continues to incur significant damages, including legal and consulting expenses, attorneys' fees, and other liability through numerous lawsuits that have been filed against MoneyGram. Under the clear and unambiguous mandatory indemnification provisions of the MSA and Exhibit D to the MSA, Capgemini must indemnify MoneyGram for these losses.

5. To make matters worse, after Capgemini utterly failed to perform its most basic security obligations, instead of cooperating with MoneyGram following the Data Incident, Capgemini has instead turned its back on MoneyGram, failed to provide assistance in dealing with the devastating aftermath of the Data Incident, and refused to acknowledge its indemnity obligations or meet and confer as required under the parties' agreement.

6. MoneyGram files this suit due to Capgemini's failure to recognize its contractual indemnity obligations and refusal to attempt to resolve in good faith MoneyGram's demands for indemnity.

II. THE PARTIES

7. Plaintiff MoneyGram is a corporation organized under the laws of Delaware with its principal place of business in Dallas, Texas. MoneyGram is a global money transfer service that allows people to send money to and from select countries. MoneyGram contracted with Capgemini to receive certain services that form the basis of this lawsuit.

8. Defendant Capgemini is a corporation organized under the laws of the State of New Jersey with its principal place of business in New York, New York. Capgemini is an IT services provider, which contracted with MoneyGram to provide IT services. In the course of providing

IT services to MoneyGram, Capgemini permitted the Unauthorized Third Party to gain access to MoneyGram customers' personal data.

III. JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(1). The parties are citizens of different States: MoneyGram is a citizen of Delaware and Texas, and Capgemini is a citizen of New Jersey and New York. The amount in controversy exceeds $75,000, exclusive of interest and costs.

10. An actual case or controversy exists within the jurisdiction of this Court pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202. On November 27, 2024, MoneyGram sent Capgemini a letter providing notice under the MSA of certain lawsuits filed against MoneyGram arising out of the Data Incident, and demanding indemnity for all losses, costs, and expenses resulting from those lawsuits. Capgemini acknowledged receipt and agreed to review the letter, but did not respond to the demand. On December 20, 2024, MoneyGram sent Capgemini an additional letter demanding indemnity for additional damages resulting from the Data Incident and seeking to schedule a pre-suit settlement meeting pursuant to Section 12.25.1 of the MSA to attempt in good faith to resolve MoneyGram's claims for indemnity. On January 8, 2025, Capgemini acknowledged receipt and indicated it would provide a response, but never did. Despite follow-up from MoneyGram, as of the date of this complaint, Capgemini has not responded to MoneyGram's demand for indemnity or request to conduct a pre-suit settlement meeting.

11. An actual case or controversy further exists because MoneyGram alleges that Capgemini breached the MSA and owes contractual indemnity to MoneyGram for all losses resulting from the Data Incident.

12. This Court has personal jurisdiction over MoneyGram and Capgemini because the parties agreed in the MSA to the personal jurisdiction of the State of Texas.

13. Venue is proper in this judicial district because the MSA requires that any proceedings involving the MSA occur in Dallas County, Texas.

IV. THE FACTS

A. Capgemini agrees to provide a service desk to handle and resolve MoneyGram's technology-related incidents and requests.

14. On August 20, 2020, MoneyGram and Capgemini entered into the MSA, which contemplated that Capgemini would provide certain services to MoneyGram as more fully described in a statement of work that the parties would execute in connection with the MSA. The latest and current statement of work between the parties pursuant to the MSA became effective September 2, 2023 and is scheduled to terminate on September 2, 2026 ("SOW"), if not otherwise terminated earlier.

15. The SOW details the specific suite of services that Capgemini agreed to provide to MoneyGram. As relevant here, Capgemini agreed through the SOW to provide personnel, facilities, and infrastructure to record, respond to, resolve, and report IT-related incidents and service requests by MoneyGram personnel through a service desk based in India ("Service Desk"). Through the Service Desk, Capgemini was required to make initial assessments of MoneyGram personnel's inquiries, log all such inquiries in MoneyGram's IT services management ("ITSM") platform, and either resolve them where technically possible or escalate them pursuant to a process outlined in the SOW.

16. Because Capgemini would be both accessing portions of the MoneyGram digital environment and receiving and processing personal data of MoneyGram customers in the course of providing its Service Desk services, the parties also entered into a Data Processing and Data

Security Addendum, which is Exhibit D to the MSA ("Data Security Addendum"). The Data Security Addendum requires that Capgemini comply with all applicable data protection laws governing the use of MoneyGram customers' personal data.

17. In addition, the Data Security Addendum outlines Capgemini's obligations related to the processing of customers' personal data, including keeping and maintaining personal data in strict confidence, training employees and representatives on how to handle personal data, and not directly or indirectly disclosing or providing access to personal data to any unauthorized persons.

18. Section 2.3 of the Data Security Addendum states, in relevant part, that Capgemini "agrees and covenants that it shall: (a) keep and maintain all Customer Personal Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure … (c) use and disclose Customer Personal Data solely and exclusively for the purposes for which the Customer Personal Data, or access to it, is provided pursuant to the terms and conditions of this Addendum and Agreement … and (d) not directly or indirectly, disclose, delete, or provide access to, Customer Personal Data to any person other than its authorized employees and representatives, without [MoneyGram's] prior written consent or as required by applicable Data Protection Laws."

19. Pursuant to the Data Security Addendum, Capgemini is also required to take certain steps to secure personal data and implement procedures to handle Security Breaches.[2] More specifically, Section 6.1 of the Data Security Addendum requires that Capgemini implement

[2] The Data Security Addendum defines "Security Breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed on systems under the direct control of [Capgemini]." "Customer Personal Data" is defined as any "data that identifies, relates to, is capable of being associated with, or could reasonably be linked to an identified or identifiable natural person or household" that is "provided to, or accessed by, [Capgemini] by or at the direction of [MoneyGram]," and that Capgemini processes on MoneyGram's behalf.

appropriate technical and organizational measures accepted in the industry to protect customers' personal data from unauthorized access, acquisition, and disclosure.

20. Additionally, Section 7 of the Data Security Addendum requires that Capgemini implement certain measures in case of a Security Breach. No later than 24 hours after becoming aware of a Security Breach, Capgemini must notify MoneyGram and provide, among other information, details of the breach, such as the number of impacted persons; the risk that the breach is likely to present to impacted persons; and security and mitigation steps taken in response to the breach. This provision further requires Capgemini to fully cooperate with MoneyGram's handling of the Security Breach, including by providing access to information and facilities, facilitating interviews with the persons involved, making all relevant records available, and assisting with any investigation into the Security Breach.

21. The MSA contains mandatory indemnification provisions governing the circumstances under which one party must indemnify the other party for all losses resulting from specified events.

22. Under Section 8.2 of the MSA, Capgemini agreed to indemnify MoneyGram for all losses, costs, expenses—including reasonable attorneys' fees—penalties, fines, judgments, settlements, damages, and liabilities resulting from, among others, Capgemini's breach of the Data Security Addendum. Section 8.2 of the MSA provides in full:

> ***Indemnification***. *Each Party ("the Indemnifying Party") agrees to indemnify, defend, and hold harmless the other Party, their respective affiliates, and their respective employees, officers, directors, and other representatives (collectively, the "Indemnified Party") from and against any and all losses, costs, expenses (including reasonable fees and expenses for attorneys, experts, and consultants, and interest), penalties, fines, judgments, settlements, damages (of all types including special damages), or liabilities, including legal fees, costs, and expenses (collectively "Losses"), suffered or incurred by any of them in connection with any claim, cause of action, or other legal assertion, brought or threatened to be brought in a legal proceeding by a third party (who is not an affiliate or representative of*

> *the Indemnified Party), or any investigation, examination, or proceeding of a governmental agency (each a "Claim"), where such Claim is based on allegations as to any of the following: (i) a breach of the Indemnifying Party's representations and warranties under the Agreement; (ii) the gross negligence or willful misconduct of the Indemnifying Party; or (iii) any breach of* ***Exhibit D*** *(DATA PROCESSING AND DATA SECURITY ADDENDUM[])] resulting from the negligent acts or omissions of the Indemnifying Party. The Indemnified Party will give prompt notice of any Claims to the Indemnifying Party. An Indemnified Party may participate in the defense of any Claims by counsel of its own choosing, at its cost and expense. Neither Party will settle any Claims without the other Party's prior written approval, which will not be unreasonably withheld. The remedies in this Section are not exclusive and do not limit any other remedies a party may have under the Agreement, Applicable Law, or otherwise.*

23. Section 9 of the Data Security Addendum contains a mandatory indemnification provision, separate from and in addition to Section 8.2 of the MSA, in which Capgemini agreed to indemnify MoneyGram for all claims, liability, costs, fines, and expenses—including legal fees—incurred by MoneyGram arising from or in connection with Capgemini's unauthorized processing of customer's personal data, Capgemini's breach of the Data Security Addendum, and a Security Breach as defined in the Data Security Addendum. Section 9 of the Data Security Addendum provides in full:

> ***Indemnification****. In addition to the indemnification obligations set forth in Section [8] of the [MSA], [Capgemini] will indemnify and hold harmless [MoneyGram] for all claims and proceedings and all liability, costs, fine[s] and expenses (including reasonable legal fees) incurred by [MoneyGram] arising from or in connection with (i) unauthorized Processing of Customer Personal Data by [Capgemini], its employees or Subprocessors, (ii) [Capgemini's] failure to comply with its obligations under this Addendum, or (iii) a Security Breach.*

24. The scope of indemnification in both Section 8.2 of the MSA and Section 9 of the Data Security Addendum thus collectively encompass any and all losses, costs, expenses (including reasonable fees and expenses for attorneys, experts, and consultants, and interest), penalties, fines, judgments, settlements, damages (of all types including special damages), and claims, proceedings, liabilities, including legal fees, costs, and expenses (hereinafter, collectively,

"Losses") resulting or arising from any of the specified events giving rise to a claim for indemnification.

B. Capgemini's service desk causes data breach that results in unauthorized access to MoneyGram customers' personal information.

25. Between September 20 and 22, 2024, Capgemini's Service Desk permitted the Unauthorized Third Party to access MoneyGram customers' personal information.

26. On September 20, 2024, the Unauthorized Third Party, pretending to be MoneyGram's then-former CFO, called the Service Desk twice requesting to reset the password and multi-factor authentication for his MoneyGram employee account. Work instructions specifically required Capgemini to authenticate the identity of the person submitting such a request by obtaining correct answers to multiple knowledge factor prompts. Importantly, those work instructions further provided that, in the event a person was unable to authenticate via multiple knowledge factor prompts, Capgemini was required to contact the requester's direct manager via email, disclosing that a reset request was received and that the person submitting that request was unable to authenticate their identity.

27. Over the following few hours, the same Capgemini analyst repeated similarly erroneous resets for the MoneyGram employee accounts associated with three other employees. In each instance, the Unauthorized Third Party failed to properly authenticate, providing incorrect answers to knowledge factor prompts. In fact, in one instance, the Unauthorized Third Party repeatedly provided an incorrect answer to one knowledge factor prompt. Instead of terminating the call and documenting the unsuccessful reset attempt—the procedure required of Capgemini by the work instructions developed pursuant to the SOW—the Capgemini analyst seemed to coach the Unauthorized Third Party toward the correct answer.

28. Here, the Unauthorized Third Party was unable to answer basic questions over the phone, such as the email address associated with the account. And when asked to identify his supervisor, it took the Unauthorized Third Party nearly twenty seconds to name MoneyGram's head of IT (who is not the CFO's supervisor).

29. Over the course of approximately four hours, Capgemini wrongly reset the MoneyGram employee account usernames and multi-factor authentication.

30. Despite the Unauthorized Third Party's failure to authenticate his identity, Capgemini granted the Unauthorized Third Party's requests to reset the password and multi-factor authentication to MoneyGram's former CFO's employee account. Additionally, at no point did Capgemini contact the purported requester's direct manager, as required by applicable work instructions.

31. As a result, the Unauthorized Party gained access to MoneyGram's secure network and acquired personal data belonging to MoneyGram customers, including names, contact information (e.g., phone numbers, email addresses, and postal addresses), dates of birth, copies of government-issued identification documents, bank account numbers, transaction information, and for a limited number of customers, Social Security numbers and criminal investigation information.

32. Immediately upon discovering the Data Incident, MoneyGram launched an investigation and completely shut down its entire global payments network for approximately six days in order to contain the data breach, leaving customers unable to transfer or access their funds. After hiring an external cybersecurity expert and through coordination with U.S. law enforcement, MoneyGram fully resumed its operations as of September 25, 2024.

C. MoneyGram incurred and continues to incur losses as a result of the Data Incident for which Capgemini refuses to provide indemnity.

33. MoneyGram's Losses as a result of the Data Incident are significant and ongoing.

34. As a direct result of the Data Incident, MoneyGram completely shut down its entire global payments network, cutting off any revenue to MoneyGram for a period of approximately six days.

35. MoneyGram was also forced to hire an external cybersecurity technology consultant, a law firm, and several other service providers to investigate the Data Incident and provide incident response, business resumption, and various other necessary support services. The lengths of engagement of these external resources vary; certain external consultants provided services for approximately one month whereas others continue to support MoneyGram as it provides relevant services to affected consumers, partners, and other parties globally.

36. As of the date of this Complaint, numerous lawsuits, including putative class actions, have been filed against MoneyGram in the United States and Canada relating to and seeking damages arising out of the Data Incident. The damages asserted against MoneyGram in these lawsuits include, among others, actual, non-economic, and statutory damages, as well as pre- and post-judgment interest, attorneys' fees, costs, and punitive damages. MoneyGram has incurred and continues to incur legal expenses, including attorneys' fees, to defend against these lawsuits.

37. MoneyGram has had to meet and correspond with regulators in more than 33 States and 17 countries in order to share relevant information concerning the temporary unavailability of MoneyGram's services and impact to consumers caused by Capgemini's acts.

38. Although Capgemini is contractually bound to fully cooperate with and notify MoneyGram following any cybersecurity event and is obligated to indemnify MoneyGram for its

losses, Capgemini has wholly ignored these contractual obligations. Despite multiple demands and correspondence, Capgemini refuses to acknowledge its obligation to indemnify MoneyGram for the Losses resulting from the Data Incident or engage with MoneyGram in good faith to resolve these demands, as required by the MSA.

39. Section 12.25.1 of the MSA requires the parties to "attempt in good faith to resolve any controversy or claim arising out of or relating to [the MSA] or the Services," as defined in the MSA.

40. On November 27, 2024, MoneyGram sent Capgemini a letter providing notice of lawsuits that had been filed against MoneyGram arising out of Capgemini's breach of the Data Security Addendum. The letter further demanded indemnity from Capgemini for all losses, as defined in the MSA, and conveyed to Capgemini that MoneyGram continued to incur damages as a result of the Data Incident that may lead to additional claims for indemnity. Despite acknowledging receipt on November 27, Capgemini provided no further response to the demand.

41. Then, on December 20, 2024, MoneyGram sent an additional letter to Capgemini seeking indemnity not only for the lawsuits listed in the November 27 letter but for all damages sustained as a result of the Data Incident, which MoneyGram continues to incur. Moreover, the December 20 letter requested a pre-suit settlement meeting pursuant to Section 12.25.1 of the MSA in January 2025 relating to MoneyGram's claims for indemnity. Despite Capgemini's indication on January 8, 2025 that a response was forthcoming, no response came. MoneyGram made subsequent attempts to elicit a response from Capgemini, but Capgemini has failed to respond, much less satisfy its obligations under the MSA.

42. MoneyGram thus had no choice but to file this lawsuit in response to Capgemini's unwillingness to recognize its indemnity obligations under the MSA and refusal to attempt in good faith to resolve MoneyGram's claims for indemnity.

V. CLAIMS FOR RELIEF

First Cause of Action: Declaratory Judgment

43. MoneyGram incorporates and adopts by reference each and every allegation in the preceding paragraphs of this Complaint.

44. An actual, immediate, and justiciable controversy exists between MoneyGram and Capgemini as to the rights and obligations under the MSA and Data Security Addendum, specifically the indemnity owed to MoneyGram that Capgemini has failed and continues to fail to acknowledge.

45. MoneyGram seeks a judicial determination and declaration of its rights of indemnity from Capgemini resulting out of the Data Incident, including but not limited to a declaration that:

a. Capgemini breached the Data Security Addendum by permitting the Unauthorized Third Party to gain access to MoneyGram's digital environment and Customer Personal Data, as that term is defined by the Data Security Addendum;

b. The Data Incident constitutes a Security Breach, as defined by the Data Security Addendum; and

c. Capgemini owes contractual indemnity to MoneyGram for all Losses resulting from the Data Incident.

46. Such declarations are necessary and appropriate at this time in order to determine the respective rights, obligations, and liabilities of the parties under the MSA and Data Security Addendum.

Second Cause of Action: Breach of Contract

47. MoneyGram incorporates and adopts by reference each and every allegation in the preceding paragraphs of this Complaint.

48. The MSA is a valid, enforceable contract binding on Capgemini, and as a party to it, MoneyGram is entitled to sue for its breach. MoneyGram has met all conditions precedent to and otherwise complied with the MSA.

49. Pursuant to the MSA's Governing Law and Venue provision, Texas law governs this breach of contract claim.

50. Exhibit D to the MSA, the Data Security Addendum, imposes on Capgemini a number of obligations relating to processing customer personal data and maintaining data security, including but not limited to:

a. Keeping and maintaining all customer personal data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure (Section 2.3(a));

b. Using and disclosing customer personal data solely and exclusively for the purposes for which the customer personal data, or access to it, is provided pursuant to the terms and conditions of the Data Security Addendum and the MSA (Section 2.3(c));

c. Not directly or indirectly disclosing, deleting, or providing access to customer personal data to any person other than MoneyGram's authorized employees and representatives without MoneyGram's prior written consent or as required by applicable data protection laws (Section 2.3(d));

d. Implementing appropriate technical and organizational measures to protect customer personal data from unauthorized access, acquisition, disclosure, destruction, alteration accidental loss, misuse, or damages that are no less rigorous than accepted industry practices (Section 6.1); and

e. Notifying MoneyGram of a Security Breach without undue delay, but not later than 24 hours after Capgemini becomes aware of it, including in such notification: (1) the categories of personal data breach and the approximate number of persons to whom that personal data relates; (2) the risk the breach presents to the rights and privileges of the persons to whom that personal data relates; and (3) the steps taken by Capgemini to mitigate the impact of the breach (Section 7.1).

51. Capgemini's Service Desk violated its clear obligations to authenticate the identity of the person seeking to reset MoneyGram employee account credentials. Capgemini further violated its obligations by failing to notify MoneyGram of the Unauthorized Third Party's repeated unsuccessful reset requests. Capgemini repeated these violations for the accounts of four different MoneyGram employee accounts, permitting the Unauthorized Third Party to gain access to MoneyGram's digital environment and MoneyGram customers' personal data.

52. In causing the Data Incident, Capgemini failed to comply with its obligations under the SOW and Data Security Addendum, including but not limited to, keeping and maintaining customer personal data in strict confidence, using and disclosing personal data only for authorized purposes, and implementing appropriate measures to protect customer personal data from unauthorized disclosure and acquisition.

53. Capgemini's violations of its obligations under the Data Security Addendum constitute material breaches of the MSA.

54. MoneyGram suffered and continues to suffer actual damages as a direct and foreseeable result of MoneyGram's breach of the MSA, specifically the Data Security Addendum, including but not limited to, attorneys' fees, legal costs, lost profits, and expenses for experts and consultants.

Third Cause of Action: Contractual Indemnity

55. MoneyGram incorporates and adopts by reference each and every allegation in the preceding paragraphs of this Complaint.

56. Pursuant to Section 8.2 of the MSA and Section 9 of the Data Security Addendum, MoneyGram is entitled to indemnity from Capgemini for all Losses resulting from or arising out of the Data Incident.

57. "Losses" is defined in Section 8.2 of the MSA as "any and all losses, costs, expenses (including reasonable fees and expenses for attorneys, experts, and consultants, and interest), penalties, fines, judgments, settlements, damages (of all types including special damages), or liabilities, including legal fees, costs, and expenses."

58. The scope of indemnification in Section 9 of the Data Security Addendum further includes "all claims and proceedings and all liability, costs, fine[s] and expenses (including reasonable legal fees)."

59. As a direct and foreseeable result of Capgemini's breach of the Data Security Addendum and the Data Incident, MoneyGram has suffered Losses, including but not limited to, attorneys' fees, legal costs, lost profits, and expenses for experts and consultants.

60. MoneyGram has performed all terms, conditions, and obligations of the MSA, including the Data Security Addendum.

61. Capgemini's refusal to indemnify MoneyGram for all Losses resulting from the Data Incident is a breach of its indemnification obligations under Section 8.2 of the MSA and Section 9 of the Data Security Addendum.

62. Pursuant to Section 8.2 of the MSA and Section 9 of the Data Security Addendum, Capgemini must indemnify MoneyGram for the Losses sustained to date as well as those continuing Losses by MoneyGram as a result of Capgemini's breach of the Data Security Addendum and the Data Incident.

VI. JURY DEMAND

63. MoneyGram hereby demands a trial by jury on all issues so triable.

VII. REQUEST FOR RELIEF

MoneyGram seeks the following relief in excess of the amount required for diversity jurisdiction under 28 U.S.C. § 1332, and the entry of judgment on its claims against Capgemini as follows:

A. An order declaring that Capgemini breached the Data Security Addendum;

B. An order declaring that the Data Incident constituted a Security Breach as defined in the Data Security Addendum;

C. An order declaring that Capgemini must indemnify MoneyGram for all losses, costs, expenses, including reasonable fees and expenses for attorneys, experts, and consultants, and interest), penalties, fines, judgments, settlements, damages (of all types, including special damages), and liabilities, including legal fees, costs, and expenses, suffered and incurred by MoneyGram as a result of the Data Incident;

D. Actual damages in an amount to be determined at trial;

E. Entry of judgment awarding MoneyGram damages for all losses, costs, liability, and fees that MoneyGram incurred and will incur as a result of the Data Incident;

F. Pre- and post-judgment interest;

G. Costs of the suit incurred herein;

H. An award of attorney's fees under Texas Civ. Prac. & Rem. Code § 38.001; and

I. Such other and further relief as the Court deems proper under the circumstances.

Dated: February 27, 2025

Respectfully submitted,

O'MELVENY & MYERS LLP

/s/ Scott Drake

Scott Drake
sdrake@omm.com
Juan Antonio Solis
jasolis@omm.com
2801 North Harwood Street, Suite 1600
Dallas, Texas 75201
Telephone: +1 972 360 1900
Facsimile: +1 972 360 1901